

**REMARKS**

This Amendment is filed in response to the Office Action mailed July 3<sup>rd</sup>, 2007.  
All objections and rejections are respectfully traversed.

Claims 1-25 are pending in the case.

No claims have been amended at this time.

Claims 20-25 have been added.

***Claim Rejections - 35 U.S.C. §103***

At paragraphs 1-2 of the Office Action, claims 1-4, 9-13, and 17-19 were rejected under 35 U.S.C. §103(a) over Viswanath et al., U.S. Patent No. 6,950,435 (hereinafter “Viswanath”), in view of Milliken, U.S. Patent Publication No. 2003/0115485 (hereinafter “Milliken”).

The Applicant’s claim 11, representative in part of the other rejected claims, sets forth (emphasis added):

11. A network node, comprising:
- a central processing unit (CPU) configured to execute instructions that implement a router operating system;
  - a network interface adapted to receive a data packet;
  - a memory having a plurality of storage locations addressable by the CPU, the storage locations being configured to store:
    - (i) at least a portion of the router operating system instructions,
    - (ii) one or more data buffers for storing the received data packet,
  - and
    - (iii) a searchable data structure configured to store information associated with the received data packet; and
- a system controller coupled to the memory and the CPU, the system controller including a hardware assist (HWA) module configured to discard malicious data packets from the network node before the malicious data packets can be forwarded to the CPU for processing by the router operating system.*

Viswanath discusses a switch with a switching fabric (Fig. 1, 25) that makes “frame forwarding decisions for received packets.” *See* col. 4, lines 41-43. A flow module (Fig. 2, 44) generates hash keys based on addresses and port numbers of received packets and combines these keys to form a packet signature. *See* Fig. 4, 74. The flow module then searches a signature table and if there is a match, forwards an entry to the switching fabric, the entry for use in executing a switching decision. *See* col. 8, lines 29-34.

Milliken discusses a security router where a “[h]ash processor 310 may optionally compare generated hash value(s) to hash values of known viruses and/or worms within hash memory (320).” *See* paragraph 0060 and Fig. 5, 515. “If one or more of the generated hash values match one of the hash values of known viruses and/or worms, the hash processor may take remedial actions...[such as] dropping the packet.” *See* paragraph 0060 and Fig. 5, 550.

The Applicant respectfully urges that the combination of Viswanath and Milliken does not teach or suggest the Applicant’s claimed *“a system controller coupled to the memory and the CPU, the system controller including a hardware assist (HWA) module configured to discard malicious data packets from the network node before the malicious data packets can be forwarded to the CPU for processing by the router operating system.”*

In contrast to prior techniques that have consumed CPU processing bandwidth identifying and removing malicious packets from a system memory, the Applicant claims a novel *hardware assist (HWA) module configured to discard malicious data packets from the network node before the malicious data packets can be forwarded to the CPU for processing by the router operating system.* As the CPU is not burdened by removing such packets, the system is less susceptible to, for example, denial-of-service attacks designed to disrupt network communication by overburdening a CPU.

The Examiner agrees that Viswanath does not discuss discarding malicious packets. As such, Viswanath clearly cannot suggest discarding packets by a special HWA module that operates on packets before a malicious data packet is forwarded to the CPU.

Milliken does discuss discarding packets, but does not suggest one do so in the manner the Applicant claims. Rather than employ *a system controller coupled to the memory and the CPU, the system controller including a hardware assist (HWA) module*, Milliken simply describes a hash processor between input and output ports. See Fig. 3. There is little discussion of how the hash processor is related to the rest of the system. Thus Milliken does not appear to suggest discarding *malicious data packets from the network node before the malicious data packets can be forwarded to the CPU for processing by the router operating system*, rather than discarding by the CPU as typically done.

Accordingly, the Applicant respectfully requests reconsideration of the rejection and urges that Viswanath and Milliken are insufficient to make obvious the present claims under 35 U.S.C. §103 because of the absence of the Applicant's claimed novel *"a system controller coupled to the memory and the CPU, the system controller including a hardware assist (HWA) module configured to discard malicious data packets from the network node before the malicious data packets can be forwarded to the CPU for processing by the router operating system."*

#### *Allowable Subject Matter*


The Applicant notes that claims 7 and 14-16 have been indicated to be allowable if rewritten in independent form. The Applicant thanks the Examiner for such indication. While the Applicant currently has not rewritten these claims in independent form, the Applicant may elect to do so in subsequent prosecution of this case. The Applicant, however, present new claims that are believed to be allowable.

Should the Examiner believe telephonic contact would be helpful in the disposition of this Application, the Examiner is encouraged to call the undersigned attorney at (617) 951-2500.

In summary, all the independent claims are believed to be in condition for allowance and therefore all dependent claims that depend there from are believed to be in condition for allowance. The Applicant respectfully solicits favorable action.

Please charge any additional fee occasioned by this paper to our Deposit Account No. 03-1237.

Respectfully submitted,



James A. Blanchette  
Reg. No. 51,477  
CESARI AND MCKENNA, LLP  
88 Black Falcon Avenue  
Boston, MA 02210-2414  
(617) 951-2500